Open Access Library Journal
2025, Volume 12, e13751
ISSN Online: 2333-9721
ISSN Print: 2333-9705

Economic Models of Using Personal Information as an Economic Resource

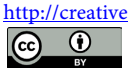
Yair Oppenheim

School of Philosophy, Linguistics and Science Studies, The Lester and Sally Antin Faculty of Humanities, Tel Aviv University, Tel Aviv-Yafo, Israel
Email: yairoppen@gmail.com

How to cite this paper: Oppenheim, Y. (2025) Economic Models of Using Personal Information as an Economic Resource. *Open Access Library Journal*, **12**: e13751.
https://doi.org/10.4236/oalib.1113751

Received: June 9, 2025
Accepted: July 18, 2025
Published: July 21, 2025

Copyright © 2025 by author(s) and Open Access Library Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/



Open Access

Abstract

The balance between individuals' interest in protecting their private information and the interests of other entities (other individuals, confidants, Internet companies, corporations, and government agencies) has been disrupted in the age of ICTs [1]. To find new points of balance, I suggest the use of game theory models, which I will now describe in two models.

Subject Areas

Development Economics

Keywords

Personal Privacy, Game Theory, Nash Equilibrium

1. Introduction

Why Use Game Theory Models

In the age of ICTs, our personal information has become a commodity in the hands of players in the commodity market [2]. Those players use individuals' personal information to maximize their profits. The said individuals, being nodes in the network, seemingly give out their private personal information for free; they provide it every time they make an online purchase, receive medical treatment, pay their taxes, search for information on Google, or browse the web for fun.

There is a debate on whether it could present personal privacy as an economic issue. I would like to say that not everyone agrees that privacy is such a great matter of concern; some scholars believe the current preoccupation with privacy to be largely an expression of older Westerners' paranoia, bringing as evidence the ease with which people share personal information on social media. According to Cal-

vin Gottlieb, "most people, when other interests are at stake, do not care enough about privacy to value it" [3].

This state of events justifies using game theory models (exemplars) to understand the rationale behind network players' decisions to violate personal privacy.

That understanding will allow us to develop alternatives that may affect the players' considerations and lead to reduced violation of personal privacy [4]. **For each model I present here, I will describe possible options that may be able to prevent or reduce personal privacy violations.**

2. Terms and Theorems

The players are selfish and rational [5]: They act out of rational considerations of gain and loss. (The considerations of ethics and sensitivity to privacy violations are reflected in the payment that players agree to pay) and solely to maximize their payoff.

Perfect information game: At every stage of the game, every player has full knowledge of all the stages of the game, of all the players' previous moves, and of the strategies each player may use during the game.

Non-cooperative game: A game in which players cannot form alliances or agree on solutions (equilibria). Each player is acting selfishly and rationally to maximize its payoff.

2.1. Model I—Putting a Price on Customers' Personal Information

Let there be a market where a network app is being sold by a monopoly (e.g., Facebook). Let us assume (without loss of generality) that the app production cost for the monopoly is 0[1], and that the price customers are willing to pay for it is distributed uniformly between [0, 1]. Provided the monopoly does not know how much customers are willing to pay for the app (the value of the app for the customers), it sets (with a probability of p) a price of p, giving us the following price function [3]: $p \cdot (1-p) = p - p^2$.

If we derive this function and set it to 0, to get the maximum value of p, we will get $1 - 2p = 0$. This means that the set a price of $\frac{1}{2}$ for a unit of the app, the monopoly's cumulative profit is $\frac{1}{4}$, and the upper median of customers gets cumulative discounts at a value of $\frac{1}{8}$.

Now, let us assume that every customer possesses information that has a direct impact on the price they will be willing to pay for the app (e.g., a list of people they want to be Facebook friends with), and that the monopoly is willing to pay $r \geq 0$ to any customer who will share that information. Any customer i who shares the information will be offered the app at a customized price of p_i. The rest of the customers will be offered the standard price p.

[1]This is reasonable because once the app has been created, its replication and distribution costs are negligible.

Based on these assumptions and conditions, we can define a game whose players are the monopoly, customers who share their personal information, and customers who do not share their personal information. It is a game with incomplete information and a common prior [3] [4], which means a game where each player has only partial knowledge of the game data. In our case, the customers do not know in advance what customized price they will be offered, and the monopoly does not know in advance the utility u_i of each customer, but it does know the distribution of customer preferences.

Description of the Game

The monopoly offers customers a discount in exchange for sharing their information. Let it be $d_i = r \cdot v_i$ (v_i being the amount of information shared by customer i).

- Every customer may decide whether to share personal information, and how much of it to share;
- The monopoly offers a standard price p to any customer j who does not share personal information, and a customized price p_i^m to any customer i who does.

Therefore, the payoff for customers who do not share personal information is $-p$, and the payoff for the monopoly in this case is $p_m = p$.

Let the price offered by the monopoly to customers who share personal information be $p_i^m(v_i) = v_i$; now, there are two options of payoff: if $r = 0$, the payoff for the customer will be $p_i = v_i$. If $r > 0$, the payoff will be $p_i = v_i + d_i$. The payoff for the monopoly will be either $p_i^m(v_i) = v_i$, or $p_i^m(v_i) = v_i - d_i$, respectively. This gives us the following game tree (See Figure 1).

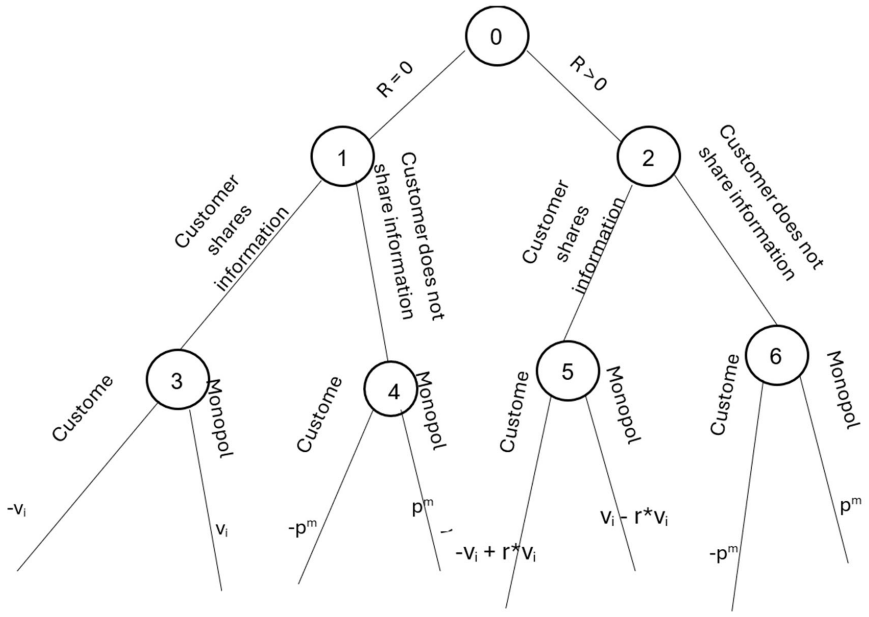


Figure 1. Game tree.

Let us analyze this game according to the Harsanyi model [5]:

The customer possesses two pieces of information: whether $r = 0$ or $r > 0$, and their personal assessment of the utility of the app for them.

The monopoly possesses two pieces of information: whether the customer is sharing their personal information, and the distribution of customer preferences (the distribution of v). It also knows that the customers who do not share their preferences know the v_i prices, so, to protect the monopoly's interest, it is necessary that $p \geq v_i$. Therefore, we can determine that eventually $p^m = 1$.

Thus, we get the following payoff matrix (See Table 1 and Table 2).

Table 1. For the customer.

		Monopoly	
		$r = 0$	$r > 0$
Customer	Shares information	$-v_i$	$-v_i + r \times v_i$
	Does not share information	-1	-1

Table 2. For the monopoly.

		Monopoly	
		$r = 0$	$r > 0$
Customer	Shares information	v_i	$v_i - r \times v_i$
	Does not share information	1	1

This game has a Bayesian equilibrium, which in this case is equivalent to a Nash equilibrium [5]. For the customers, the best strategy is to share their information to secure a price of $v_i \leq 1$, which is lower than the monopoly price $p^m = 1$. Knowing that, the monopoly will always choose $r = 0$ to make sure it gets paid at least $v_i > v_i - r \cdot v_i$. This state of events reflects typical customer interaction with monopolistic Internet companies, where individual customers provide their personal information to the Internet companies for free. It also reflects the state of the market, where the monopolies (Internet companies) get all the surplus (more than 25% above what they would have earned without the partial knowledge of customer preferences), while the customers get no surplus at all and have to pay either the full price or the exact price they were willing to pay anyway. In this model, the sharing of personal information is good for the Internet companies and bad for the customers. Furthermore, today, the use of AI technology usually allows Internet companies to obtain personal information without even having to ask for the individual's permission.

2.2. Model II—Commercializing Customers' Personal Information

An online advertiser has to align their product's price with the customers' preferences [5] [6]. Let v be the value of the advertised product unit, distributed uniformly $v = [0, 1]$. Let the advertiser's matching function be $m(x) = \frac{x^2}{2}$, with x

standing for the cost of customer communication channels[2]. This means the advertiser's profit from an advertised product is $f(v,x)=vx-\frac{x^2}{2}$.

Let there be a database manager who can provide the advertiser with the customer data it needs for a price of p for each customer i whose personal data the advertiser wants to buy. If the advertiser can obtain the personal data it needs without buying it from the database manager, it can create a customized advertising package where $x^*=v_i$ for every customer i, to achieve the optimal profit of $f^*(v_i,x^*)=v_i\cdot v_i-\frac{v_i^2}{2}=\frac{v_i^2}{2}$.

For the rest of the customers, whose personal information is not in its possession, the advertiser has to set a standard price of $x^{\wedge}$. Now it has to pick a category of customers whose personal data it will buy from the database manager; otherwise, it faces a risk of over-advertising or under-advertising. In a state of uniform distribution between [0, 1], the equilibrium strategy will be: $v=p=\frac{1}{2}$[3].

Because v_i is unknown to the advertiser, it can charge customers the price of their data p.

If the customer buys the product for p, the advertiser's matching function will be $m(v_i)=v_i^2-p$.

The break-even point is $v_i^2-p=0$, than $v_i^2=p$ thus $v_i=\sqrt{p}$. In this case, the equilibrium strategy will be:

$$F^*(v_i)=\begin{cases} v_i\geq\sqrt{p} & \text{Buy the ad} \\ v_i<\sqrt{p} & \text{Do not buy the ad}\end{cases}$$

The probability of a customer buying the product from the ad is (p – 1), based on the sealed-bid auction with entry fee model [1]. Thus, we will get:

$$F^*(p)=\frac{\left(1-\sqrt{p}\right)\cdot\left(4p+\sqrt{p}\right)+1}{3}$$

This is a concave function of p in which $F^*(0)=\frac{1}{3}$ and $F^*(1)=0$. If we derive it, we will get:

$$F'(p)=\left[\left(1-\sqrt{p}\right)\cdot\left(4p+\sqrt{p}\right)+\left(1+3p-4p^{3/2}\right)\right]'=3-6\cdot1=\sqrt{p}$$

The maximum point of the function is $p^*=\frac{1}{4}$. Therefore, the price for customers whose $v_i<\frac{1}{2}$ will be: $p^*=\frac{1}{2}-\frac{1}{4}=p^l=\frac{1}{4}-\frac{1}{2}$ while the price for customers whose $v_i\geq\frac{1}{2}$ will be: $p^h=\frac{3}{4}$.

In this state of events, the advertiser's expected profit is:

[2]Includes costs of website maintenance and online advertising (e.g., through Google Ads).

[3]See justification in the previous section.

$$F\left(\frac{1}{4}\right)=\frac{1}{3}\cdot\left(1-\frac{1}{2}\right)\cdot\left(4\cdot\frac{1}{4}+\frac{1}{2}+1\right)=\frac{1}{3}\cdot\frac{1}{2}\cdot\frac{5}{2}=\frac{5}{12}>\frac{1}{3}$$

This will make the database manager want to maximize p, based on $p\cdot\left(1-2\cdot\sqrt{p}\right)$. If we derive this function, we will get: $1=6\cdot\sqrt{p}$; therefore, for the database manager $p^d=\frac{1}{36}$.

This model shows that online advertising can guarantee advertisers an expected profit of $>\frac{1}{3}$, and that database managers can secure a revenue of $\frac{1}{16}$ for each customer whose personal data they sell. In other words, this model justifies surveillance capitalism practices of making money by using the personal information of online customers, which has been obtained for zero or near-zero price.

3. Conclusions

To conclude, in this article, I described two game theory models which illustrate how our personal information can be (and is being) used to maximize the profits of Internet companies, which exploit it for purposes of targeted advertising and niche (long tail) production.

The models discussed here show that Internet companies, which are practically monopolies, have the most to gain from violating our personal privacy.

To improve this situation, either/or all of the following should happen: one possible solution is more severe fining of confidants and Internet companies who violate personal privacy; this is the purpose of the GDPR. However, this is not enough; the paradigm of personal privacy that is founded on consent and control should be replaced by a new one that would pass the responsibility for privacy protection from the individuals, who are expected to give consent and have control over their personal information, to the Internet companies and confidants, who should be held responsible and liable for fair and proper use of the said information. Another direction is putting, by regulation, a price tag on personal information and imposing the costs on Internet companies to restrain their uncontrollable appetite for using personal information as a free resource from which they can profit. That could be done by creating an economic model of Internet company taxation based on the amount of personal privacy information the company uses [1], similar to electricity and water payments. The model will measure privacy information in kilobytes of information from each category of privacy information – for example, how many kilobytes of medical or financial information Facebook has on a particular individual user or how many kilobytes of medical information in total it has about all its users[4].

Conflicts of Interest

The author declares no conflicts of interest.

[4]The model may be progressive, like electricity and water consumption billing.

References

[1] Oppenheim, Y. (2024) Personal Privacy in the Age of the Internet. Spines, 122-135.

[2] Rajbhandari, L. and Snekkenes, E.A. (2011) Using Game Theory to Analyze Risk to Privacy: An Initial Insight. In: Fischer-Hübner, S., Duquenoy, P., Hansen, M., Leenes, R. and Zhang, G., Eds., *Privacy and Identity Management for Life*, Springer, 41-51. https://doi.org/10.1007/978-3-642-20769-3_4

[3] Gottlieb, C.C. (1996) Privacy: A Concept Whose Time Has Come and Gone. In: Lyon, D. and Computer, E.Z., Eds., *Surveillance*, *and Privacy*, University of Minnesota Press, 156.

[4] Shilov, I., Le Cadre, H. and Busic, A. (2021) Privacy Impact on Generalized Nash Equilibrium in Peer-to-Peer Electricity Market. *Operations Research Letters*, **49**, 759-766. https://doi.org/10.1016/j.orl.2021.08.001

[5] Maschler, M., Solan, E. and Zamir, S. (2013) Game Theory. Cambridge University Press. https://doi.org/10.1017/cbo9780511794216

[6] Ananthakrishnan, N., Ding, T., Werner, M., Karimireddy, S.P. and Jordan, M.I. (2024) Privacy Can Arise Endogenously in an Economic System with Learning Agents. arXiv: 2404.10767. https://doi.org/10.48550/arXiv.2404.10767